

SEALED

United States District Court

NORTHERN

DISTRICT OF

MAR 15 2016

CLERK, U.S. DISTRICT COURT

By TEXAS**In the Matter of the Search of**

(Name, address or Brief description of person, property or premises to be searched)

Electronic devices currently located at the
United States Postal Inspection Service
2400 DFW Turnpike, 3rd Floor
Dallas, Texas 75398

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**CASE NUMBER: 3:16-MJ- 341 BFI Thomas W. Brown being duly sworn depose and say:

I am a(n) Postal Inspector with the United States Postal Inspection Service (USPIS) and have reason to believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).


in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, concerning a violation of Title 18 United States code, Section(s) 1708, 1028 and 1028A. The facts to support a finding of Probable Cause are as follows:

(SEE ATTACHED AFFIDAVIT OF POSTAL INSPECTOR THOMAS W. BROWN).

Continued on the attached sheet and made a part hereof. XX Yes No

Signature of Affiant

Thomas W. Brown

Postal Inspector, USPIS

Sworn to before me, and subscribed in my presence

March 15, 2016 @ 1145
Date and Time

at

Dallas, Texas
City and State

PAUL D. STICKNEY

United States Magistrate Judge

Name and Title of Judicial Officer


Signature of Judicial Officer

ATTACHMENT A

The properties to be searched are a **blue HP 2000 Laptop, serial number BDAH7101BDD2K0F**, a **black Acer laptop SN LXR4P0214604723ABD1601**, a **black Samsung Galaxy phone in a black carrying case with an unknown serial number** and a **silver PNY 32GB thumb drive with an unknown serial number**, herein thereafter the “Devices”. The Devices are currently located at United States Postal Inspection Service, 2400 DFW Turnpike 3rd Floor, Dallas, Texas 75398. The **silver PNY 32GB thumb drive with an unknown serial number** has been in the possession of the United States Postal Inspection Service since March 16, 2015. The **blue HP 2000 Laptop, serial number BDAH7101BDD2K0F**, a **black Acer laptop SN LXR4P0214604723ABD1601** have been in the possession of the United States Postal Inspection Service since October 15, 2015, and the **black Samsung Galaxy phone in a black carrying case with an unknown serial number** has been in the possession of the United States Postal Inspection Service since February 4, 2016.

ATTACHMENT B

All records and information relating to violations of 18 U.S.C. §§ 1028(a)(1) (Fraud in Relation to Identification Documents), 1028A (Aggravated Identity Theft) and 1708 (Theft or Receipt of Stolen Mail Matter) including the following:

- a. any software enabling the creation of counterfeit checks or other financial instruments;
- b. any credit-card producing software;
- c. any check producing software;
- d. any records indicating the production of counterfeit identification documents;
- e. any internet records indicating access to bank accounts not bearing the name of Estfano Burhe or Joshua Jamar Norman;
- f. any records of internet purchases using credit accounts in a name other than Estfano Burhe or Joshua Jamar Norman;
- g. any electronic communications (including emails, "chats," or instant messages) from Estfano Burhe or Joshua Jamar Norman to possible co-conspirators regarding violations of 18 U.S.C. § 1028(a)(1), Fraud in Relation to Identification Documents, 18 U.S.C. § 1028A, Aggravated Identity Theft, or 18 U.S.C. § 1708, Receipt of Stolen Mail Matter;

- h. evidence of who used, owned or controlled the computer or storage devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, "chat," instant messaging logs, photographs, and correspondence;
- i. evidence of software that would allow others to control the computer or storage devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of any security software designed to detect malicious software;
- j. evidence of the lack of such malicious software;
- k. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- l. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or storage devices;
- m. evidence of the times the computer or storage devices were used;
- n. passwords, encryption keys, and other access devices that may be necessary to access the computer or storage devices;
- o. documentation and manuals that may be necessary to access the computer or storage devices or to conduct a forensic examination of the computer or storage devices;
- p. records of or information about Internet Protocol addresses used by the computer;

- q. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- r. contextual information necessary to understand the evidence described in this attachment.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Thomas Brown, a Postal Inspector with the United States Postal Inspection Service (USPIS), being duly sworn, depose and state the following:

INTRODUCTION

I make this affidavit in support of an application for a search warrant for data and information, for a **blue HP 2000 Laptop, serial number BDAH7101BDD2K0F, a black Acer laptop SN LXR4P0214604723ABD1601, a black Samsung Galaxy phone in a black carrying case with an unknown serial number and a silver PNY 32GB thumb drive with an unknown serial number.** As set forth herein, I respectfully submit that there is probable cause to believe that the items sought by this search warrant constitute evidence of violations of 18 U.S.C. §§ 1708, 1028 and 1028A.

I am a United States Postal Inspector and have been so employed for approximately 12 years. I am presently assigned to the Fort Worth Division Dallas External Crimes Team. As part of my duties as a Postal Inspector, I investigate financial crimes and identity theft involving the use of the U.S. Mail. I also investigate the use of the U.S. Mail to illegally send and receive documents that contain false or misappropriated identification used to obtain credit cards, loans, or other items of value. As part of this assignment, I received formal training from the U.S. Postal Inspection Service and training through contact with experts from various law enforcement agencies. I have received training in the enforcement of laws and methods of investigation. I have

conducted and participated in criminal investigations utilizing various methods of investigation.

As a federal agent, your affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

The properties to be searched are a **blue HP 2000 Laptop, serial number BDAH7101BDD2K0F, a black Acer laptop SN LXR4P0214604723ABD1601, a black Samsung Galaxy phone in a black carrying case with an unknown serial number and a silver PNY 32GB thumb drive with an unknown serial number**, hereinafter the **“Devices.”** The **Devices** are currently located at United States Postal Inspection Service, 2400 DFW Turnpike 3rd Floor, Dallas, Texas 75398.

The applied-for warrant would authorize the forensic examination of the **Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

FACTS SUPPORTING PROBABLE CAUSE

Since the affidavit is being submitted for the limited purpose of supporting a search warrant, I have not included each and every known fact concerning this investigation. I have set forth only the facts believed necessary to establish probable cause to obtain said warrant. Where statements of others are set forth in this affidavit, they are set forth in substance and are not verbatim. The information contained in this affidavit is based on my personal observations and experiences, in addition to

information obtained by other law enforcement agents, witnesses and documents.

Specifically, based upon all of the facts and information set forth in this affidavit, your affiant respectfully states that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1708, 1028 and 1028A, can be found in the computer hard drives and electronic media previously seized pursuant to the arrest of Estfano Mashai Burhe (BURHE) on March 11, 2015 and January 30, 2016, and Joshua Jamar Norman (NORMAN) on March 11, 2015.

As is specified below, the subjects have been known to facilitate the use and possession of fraudulent or counterfeit documents in violation of federal law, and use of personal information; and evidence found in possession of the subjects is consistent with the use of unlawfully obtained identification documents and use of unlawfully obtained identification information. In your affiant's training and experience, the computer hard drives and electronic media recovered by law enforcement may contain evidence, fruits, and instrumentalities of violations of federal law as specified herein and in Attachment B.

On March 11, 2015, a Dallas County Sheriff's Deputy conducted a traffic stop on a silver Honda Accord bearing Texas License plate BDH8186 for speeding in Dallas, Texas. While making contact with the driver, BURHE, the Deputy could smell a strong odor of marijuana coming from the vehicle. BURHE did not have a valid Texas Driver License and a warrant check showed BURHE had outstanding warrants. A warrant check of the front passenger, NORMAN, showed he also had outstanding warrants.

During a pat down search of BURHE, Deputies noticed BURHE had several credit cards with different people's names on them and a Texas CDL Driver License not

belonging to BURHE. Once BURHE and NORMAN were secured, the Deputies searched BURHE's vehicle due to a strong smell of marijuana. Inside the vehicle, Deputies located more credit cards not in BURHE's or NORMAN's names and large amounts of stolen United States Mail from apartment complexes in Dallas and Richardson. In the driver's side door of BURHE's vehicle, Deputies found two temporary Texas Driver Licenses with BURHE's picture, but in the names of T.S. and C.A. Located with the fraudulent temporary Texas Driver License in the name of C.A. was a check made payable to C.A. Deputies also located a box containing numerous credit cards not in BURHE's name and a silver PNY 32GB thumb drive inside the same box. Deputies also recovered a blue HP 2000 Laptop, serial number BDAH7101BDD2K0F and a black Acer laptop SN LXR4P0214604723ABD1601. BURHE was arrested by Dallas County Sheriff's Deputies and charged with Fraudulent Use/Possession of Identifying Items less than five, Possession of Substance in Penalty Group 1 and outstanding warrants. NORMAN was arrested for outstanding warrants. Deputies seized the items located in BURHE's vehicle and retained it as evidence.

On January 30, 2016, Irving Police Officers were dispatched to a suspicious vehicle at 6300 North MacArthur Boulevard, Irving, Texas. The caller mentioned a male carrying a trash can from the mail center to a white U-Haul bearing Arizona License Plate AG52500. Upon arrival, officers observed numerous open letters on the ground near the driver's side door and stacks of mail inside the vehicle. Irving Police identified the driver of the vehicle as BURHE. BURHE gave officers consent to search his person. Inside his front coin pocket in his jeans, officers located 0.4 grams of methamphetamine.

BURHE was charged with Possession of a Controlled Substance Penalty Group 1 <1gram. Inside BURHE's left front pocket, officers located a MasterCard gift card and a temporary Texas Driver License in the name of A.H.

During the search of the vehicle, officers located voluminous amounts of stolen mail from apartment complexes in Dallas, Plano and Irving, Texas. They also located a black Samsung Galaxy phone in a black carrying case with an unknown serial number. BURHE claimed the mail belonged to him, even though the mail was not addressed to him. All of the items were seized and retained as evidence.

TECHNICAL TERMS

In order to ensure that agents search only the computer files described in this search warrant, Affiant seeks authorization to permit employees of the United States Postal Inspection Service National Computer Crime Lab to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those computer files described in Attachment B, the following procedures have been implemented:

- a. The warrant will be presented to personnel of the U.S. Postal Inspection Service National Computer Crime Lab, hereinafter referred to as "systems administrators" who will be directed to isolate those files described in detail in Attachment B;
- b. In order to minimize any disruption of computer service, the systems administrator and law enforcement personnel trained in the operation of computers will create an exact duplicate of the files described in

Attachment B;

- c. The system administrator will provide the exact duplicate in hard copy and an electronic form of the files described in Attachment B and all information stored in those files to the Postal Inspector or Agent who serves this search warrant;
- d. Law enforcement personnel will thereafter review the information stored in the files received from the systems administrator and then identify and copy the information contained in those files which are authorized to be further copied by this search warrant; and
- e. Law enforcement personnel will then seal the original duplicate of the files received from the systems administrator and will not further review the original duplicate absent an order of the Court.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

There is probable cause to believe that things that were once stored on the **Devices** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after

they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes

automatically downloaded into a temporary Internet directory or “cache.”

Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Devices** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Devices** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for

“indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

Based upon the information above, your affiant believes that there is probable cause that within the **Devices** described herein, there exists fruits, instrumentalities and evidence of violations of 18 U.S.C. §§ 1708, 1028 and 1028A.

I respectfully request that a search warrant be issued, authorizing me with the appropriate assistance from other qualified Federal law enforcement or personnel duly authorized by federal law enforcement agents, to search and forensically examine the **Devices** specified in Attachment A, located in USPIS' custody at 2400 DFW Turnpike 3rd Floor, Dallas, Texas 75398 and therein search for and seize the items as set forth in Attachment B.

Respectfully submitted,



Thomas W. Brown
U.S. Postal Inspector

Subscribed and sworn to before me on this the 15 day of March, 2016



PAUL D. STICKNEY
United States Magistrate Judge
Northern District of Texas